大阪広域環境施設組合情報セキュリティ管理規程

平成27年３月30日達第３号

最終改正：令和元年７月23日

目　次

第１章　総則

（目的）

第１条　この規程は、行政事務における情報通信の技術の適正な利用の推進に関する規程（平成27年達第２号。以下「情報通信技術適正利用推進規程」という。）第８条に規定する情報システム及び情報システムにより処理される情報、同規程第13条に規定する通信ネットワーク及び通信ネットワークにより伝達される情報その他の本組合が保有する情報資産に関する情報セキュリティの確保のために必要な事項を定めるものとする。

（定義）

第２条　この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1)　情報セキュリティ　情報資産の機密を保持し、情報資産の正確性及び完全性を維持し、並びに定められた範囲での利用可能な状態を維持することをいう。

(2)　情報資産　情報システム及び通信ネットワークの開発及び運用管理に係るファイル（データを記録している電磁的記録をいう。以下同じ。）及

びドキュメント（情報システムの設計書、操作手引書、プログラムリスト、ネットワーク構成図その他の電子計算機の運用に関する文書をいう。）、情報システム及び通信ネットワークで取り扱うデータに係るファイル並びに情報システム及び通信ネットワークを構成する機器をいう。

(3)　情報セキュリティポリシー　この規程及び第７条に規定する情報セキュリティ対策基準をいう。

(4)　情報セキュリティ対策　情報セキュリティを確保するために実施する各種の対策をいう。

(5)　電子計算機処理　電子計算機を使用して行われる情報の入力、蓄積、編集、加工、修正、更新、検索、消去、出力又はこれらに類する処理をいう。

(6)　電磁的記録　電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。

(7)　データ　電子計算機処理に係る情報で媒体に記録されているものをいう。

(8)　情報システム　情報通信技術適正利用推進規程第２条第１号に規定する情報システムをいう。

(9)　通信ネットワーク　情報通信技術適正利用推進規程第２条第２号に規定する通信ネットワークをいう。

(10)　課　大阪広域環境施設組合公文書管理条例施行規則（平成26年規則第６号。以下「公文書管理条例施行規則」という。）第７条第４項に規定する課（工場を含む。）をいう。

（職員の責務）

第３条　職員は、情報セキュリティの重要性を十分に認識し、情報セキュリティポリシーを遵守するとともに、大阪広域環境施設組合個人情報保護条例（平成27年条例第９号）その他の関連する法令等を遵守し、情報資産を適切に管理しなければならない。

第２章　情報セキュリティに係る体制

（統括情報セキュリティ責任者等の設置等）

第４条　本組合に統括情報セキュリティ責任者を置き、事務局長をもって充てる。

２　本組合に副統括情報セキュリティ責任者を置き、総務部長をもって充てる。

３　統括情報セキュリティ責任者は、本組合における情報セキュリティを統括し、情報セキュリティ対策の統一的な実施に必要な指導、助言又は調整を行う。

４　副統括情報セキュリティ責任者は、統括情報セキュリティ責任者を補佐する。

５　IT管理者（情報通信技術適正利用推進規程第４条第１項に規定するIT管理者をいう。以下同じ。）は、統括情報セキュリティ責任者の命を受けて、本組合における各情報システムの開発及び運用状況、データの管理状況、通信ネットワークの利用状況等を把握し、情報セキュリティ対策が適切かつ確実に実施されるよう必要な助言又は調整を行う。

（課情報セキュリティ責任者の設置等）

第５条　課における情報セキュリティ対策の適正な実施を推進するため、課に課情報セキュリティ責任者を置く。

２　課情報セキュリティ責任者は、課長等をもって充てる。

３　課情報セキュリティ責任者は、統括情報セキュリティ責任者の命を受けて、その所管に係る情報資産に関し情報セキュリティ対策が適切かつ確実に実施されるよう、必要な措置を講じなければならない。

第３章　情報セキュリティ対策

（情報資産の分類）

第６条　課情報セキュリティ責任者は、課が保有する情報資産をその内容に応じて分類し、重要性に応じた情報セキュリティ対策を実施しなければならな

い。

（情報セキュリティ対策基準の作成）

第７条　統括情報セキュリティ責任者は、本組合における情報資産の取扱いについて遵守すべき事項及び情報セキュリティ対策の実施に関する統一的な規準を定めるため、情報セキュリティ対策基準を作成しなければならない。

（情報セキュリティ実施手順の作成）

第７条の２　課情報セキュリティ責任者は、その所管する情報システム又は通信ネットワークにおける情報セキュリティ対策の実施に関し必要となる事項を定めるため、情報セキュリティ実施手順を作成し、統括情報セキュリティ責任者の承認を得なければならない。

（ソフトウェアライセンスの管理）

第８条　課情報セキュリティ責任者は、課において使用するソフトウェアのライセンス（当該ソフトウェアに係る使用許諾契約により認められた当該ソフトウェアを使用する権利をいう。）を適切に管理しなければならない。

２　課情報セキュリティ責任者は、ソフトウェアライセンスの管理状況を適宜調査し、その内容を定期的に統括情報セキュリティ責任者に報告しなければならない。

３　統括情報セキュリティ責任者は、前項の規定による報告を受けた場合において、必要があると認めるときは、必要な措置が適切に講じられるよう指導及び監督を行わなければならない。

４　ソフトウェアライセンスの管理の方法その他必要な事項は、統括情報セキュリティ責任者が定める。

（業務の委託）

第９条　課情報セキュリティ責任者は、電子計算機処理業務の全部又は一部を委託しようとする場合は、データの秘密保持に関する事項、契約または協定に違反したときの契約解除又は指定の取消しに関する事項、損害賠償に関する事項その他統括情報セキュリティ責任者が定める事項を委託契約書又は協

定書に明記するなど、情報資産の適切な管理のために必要な措置を講じなければならない。

（事故発生時の措置）

第10条　IT管理者は課が保有する情報資産に漏えい、滅失、き損、改ざん等の事故が発生したときは、直ちに、その状況を調査するとともに、当該事故の内容を課情報セキュリティ責任者に報告しなければならない。

２　課情報セキュリティ責任者は、前項の規定による報告を受けたときは、直ちに必要な措置を講ずるとともに、事故の内容及び講じた措置を統括情報セキュリティ責任者に報告しなければならない。

３　統括情報セキュリティ責任者は、前項の規定による報告を受けたときは、再発防止のために必要な措置が適切に講じられるよう指導及び監督を行わなければならない。

第４章　検証及び見直し

（情報セキュリティ検査の実施）

第11条　統括情報セキュリティ責任者は、本組合において情報セキュリティポリシーが遵守され、情報セキュリティ対策が適切かつ確実に実施されているかどうかを検証するため、定期的に検査を実施しなければならない。

２　統括情報セキュリティ責任者は、前項に規定する検査のほか、必要と認めるときは随時に検査を行うことができる。

３　統括情報セキュリティ責任者は、前２項に規定する検査（以下「情報セキュリティ検査」という。）の結果に基づき、必要があると認めるときは、講ずべき改善措置の内容を定めなければならない。

４　課情報セキュリティ責任者は、前項の規定により統括情報セキュリティ責任者が定める改善措置を適切かつ確実に実施しなければならない。

５　情報セキュリティ検査の実施方法その他必要な事項は、統括情報セキュリティ責任者が定める。

（見直しの実施）

第12条　統括情報セキュリティ責任者は、情報セキュリティをめぐる情勢の変化等を勘案し、及び情報セキュリティ検査の結果を踏まえ、適宜情報セキュリティポリシーに検討を加え、必要があると認めるときは、これを変更しなければならない。

２　課情報セキュリティ責任者は、前項の規定に準じて、情報セキュリティ実施手順に検討を加え、必要があると認めるときは、これを変更しなければならない。

第５章　データ管理

（データの管理）

第13条　課情報セキュリティ責任者は、データの取扱いに当たっては、漏えい、滅失、き損、改ざん並びに不正な利用及び提供等を防止するなど、適切に管理しなければならない。

２　データの管理の方法その他必要な事項は、統括情報セキュリティ責任者が定める。

第６章　雑則

（施行の細目）

第14条　この規程の施行に関し必要な事項は、統括情報セキュリティ責任者が定める。

附　則

この規程は、令達の日から施行する。

附　則（平成31年２月22日達第１号）

この規程は、平成31年３月１日から施行する。

附　則（令和元年７月23日達第１号）

この規程は、令和元年10月１日から施行する。